

**FULL VERSION OF PENDING CLAIMS**

1        Claim 1 (Currently Amended): A cipher strength estimating device for estimating a  
2        strength of a ciphertext which is a transformed text obtained at a final round of a transformation  
3        process including: receiving a plaintext; transforming the plaintext using, as a parameter, a  
4        session key calculated from a key for use in encryption; and repeatedly further transforming the  
5        resulting transformed text which is the plaintext thus transformed to perform stepwise  
6        encryption,

7        the cipher strength estimating device comprising an untransformed text calculating unit  
8        and a control unit, the untransformed text calculating unit comprising a session key prospect  
9        calculating section and an untransformed text calculating unit body, wherein:

10       the untransformed text calculating unit is operative to receive, as inputs thereto, the  
11       plaintext and one of the ciphertext obtained at the final round of the transformation process and a  
12       putative transformed text presumed to be a transformed text obtained at a certain intermediate  
13       round;

14       the session key prospect calculating section is operative to: calculate one session key  
15       prospect presumed to be equivalent to the session key to be used at a relevant round of  
16       transformation by using the plaintext and one of the ciphertext and the putative transformed text  
17       or output uncalculability identifier data indicative of inability to calculate when the calculation is  
18       impossible; and optionally calculate another session key prospect for the relevant round which is  
19       different from the session key prospect already outputted in response to receipt of recalculation  
20       request data requesting recalculation;

21       the untransformed text calculating unit body is operative to: calculate a putative  
22       untransformed text presumed to be equivalent to an untransformed text which is not transformed

23 yet at the relevant round based on the session key prospect and one of the ciphertext and the  
24 putative transformed text; and output the putative untransformed text as an output of the  
25 untransformed text calculating unit; and

26 the control unit is operative to: input the plaintext and one of the ciphertext obtained at  
27 the final round of the transformation process and the putative transformed text obtained at the  
28 certain intermediate round, which make a pair, to the untransformed text calculating unit; receive  
29 the putative untransformed text outputted; and repeatedly further input the putative  
30 untransformed text as a putative transformed text for a round immediately preceding the relevant  
31 round to the untransformed text calculating unit together with the plaintext; and optionally output  
32 the recalculation request data to the session key prospect calculating section in response to  
33 receipt of the uncalculability identifier data outputted from the session key prospect calculating  
34 section to cause the session key prospect calculating section to again calculate said another  
35 session key prospect for the immediately preceding round, and then output the putative  
36 untransformed text based on said another session key prospect.

1 Claim 2 (Original): A cipher strength estimating device for estimating a strength of a  
2 ciphertext which is a transformed text obtained at a final round of a transformation process  
3 including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key  
4 calculated from a key for use in encryption; and repeatedly further transforming the resulting  
5 transformed text which is the plaintext thus transformed to perform stepwise encryption,

6 the cipher strength estimating device comprising an untransformed text calculating unit  
7 and a control unit, the untransformed text calculating unit comprising a session key prospect  
8 calculating section and an untransformed text calculating unit body, wherein:

the untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round;

the session key prospect calculating section is operative to: dynamically create a condition for use in calculating one session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by using the plaintext and one of the ciphertext and the putative transformed text; calculate the session key prospect based on the condition thus created or output uncalculability identifier data indicative of inability to calculate when the calculation is impossible; and optionally calculate another session key prospect for the relevant round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation;

the untransformed text calculating unit body is operative to: calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and

the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the untransformed text calculating unit; receive the putative untransformed text outputted; repeatedly further input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the untransformed text calculating unit together with the plaintext; and optionally output the

32 recalculation request data to the session key prospect calculating section in response to receipt of  
33 the uncalculability identifier data outputted from the session key prospect calculating section to  
34 cause the session key prospect calculating section to again calculate said another session key  
35 prospect for the immediately preceding round and then output the putative untransformed text  
36 based on said another session key prospect.

1 Claim 3 (Currently Amended): A cipher strength estimating device for estimating a  
2 strength of a ciphertext which is a transformed text obtained at a final round of a transformation  
3 process including: receiving a plaintext; transforming the plaintext using, as a parameter, a  
4 session key calculated from a key for use in encryption; and repeatedly further transforming the  
5 resulting transformed text which is the plaintext thus transformed to perform stepwise  
6 encryption,

7 the cipher strength estimating device comprising an untransformed text calculating unit  
8 and a control unit, the untransformed text calculating unit comprising a session key prospect  
9 calculating section and an untransformed text calculating unit body, wherein:

10 the untransformed text calculating unit is operative to receive, as inputs thereto, the  
11 plaintext and one of the ciphertext obtained at the final round of the transformation process and a  
12 putative transformed text presumed to be a transformed text obtained at a certain intermediate  
13 round;

14 the session key prospect calculating section is operative to: dynamically create conditions  
15 for use in calculating a session key prospect presumed to be equivalent to the session key to be  
16 used at a relevant round of transformation by using the plaintext and one of the ciphertext and  
17 the putative transformed text; calculate the session key prospect based on the conditions thus

18 created or identify inability to calculate when inconsistency is found between certain two of the  
19 conditions and then output uncalculability identifier data indicative of inability to calculate; and  
20 optionally calculate another session key prospect for the relevant round which is different from  
21 the session key prospect already outputted in response to receipt of recalculation request data  
22 requesting recalculation;

23 the untransformed text calculating unit body is operative to calculate a putative  
24 untransformed text presumed to be equivalent to an untransformed text which is not transformed  
25 yet at the relevant round based on the session key prospect and one of the ciphertext and the  
26 putative transformed text; and output the putative untransformed text as an output of the  
27 untransformed text calculating unit; and

28 the control unit is operative to: input the plaintext and one of the ciphertext obtained at  
29 the final round of the transformation process and the putative transformed text obtained at the  
30 certain intermediate round, which make a pair, to the untransformed text calculating unit; receive  
31 the putative untransformed text outputted; repeatedly further input the putative untransformed  
32 text as a putative transformed text for a round immediately preceding the relevant round to the  
33 untransformed text calculating unit together with the plaintext; and optionally output the  
34 recalculation request data to the session key prospect calculating section in response to receipt of  
35 the uncalculability identifier data outputted from the session key prospect calculating section to  
36 cause the session key prospect calculating section to again calculate said another session key  
37 prospect for the immediately preceding round and then output the putative untransformed text  
38 based on said another session key prospect.

1           Claim 4 (Currently Amended): A cipher strength estimating device for estimating a  
2 strength of a ciphertext which is a transformed text obtained at a final round of a transformation  
3 process including: receiving a plaintext; transforming the plaintext using, as a parameter, a  
4 session key calculated from a key for use in encryption; and repeatedly further transforming the  
5 resulting transformed text which is the plaintext thus transformed to perform stepwise  
6 encryption,

7           the cipher strength estimating device comprising a first untransformed text calculating  
8 unit, a second untransformed text calculating unit, and a control unit, the first untransformed text  
9 calculating unit comprising an untransformed text calculating unit body and a first session key  
10 prospect calculating section, the second untransformed text calculating unit comprising a second  
11 session key prospect calculating section, wherein:

12           the first untransformed text calculating unit is operative to receive, as inputs thereto, the  
13 plaintext and one of the ciphertext obtained at the final round of the transformation process and a  
14 putative transformed text presumed to be a transformed text obtained at a certain intermediate  
15 round;

16           the second untransformed text calculating unit is operative to receive, as inputs thereto,  
17 the plaintext and one of the ciphertext obtained at the final round of the transformation process  
18 and a putative transformed text presumed to be a transformed text obtained at a certain  
19 intermediate round;

20           the first session key prospect calculating section is operative to: conduct brute-force  
21 search for the session key to be used at a certain round of transformation by using the plaintext  
22 and one of the ciphertext and the putative transformed text; calculate one session key prospect

presumed to be equivalent to the session key to be used at said certain round of transformation or output uncalculability identifier data indicative of inability to calculate when the calculation is impossible; and optionally calculate another session key prospect for said certain round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation;

the second session key prospect calculating section is operative to: dynamically create plural conditions for use in calculating a session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by higher order differential cryptanalysis using the plaintext and one of the ciphertext and the putative transformed text; and calculate one session key prospect based on the conditions thus created or identify inability to calculate when inconsistency is found between certain two of the conditions and then output uncalculability identifier data indicative of inability to calculate;

the untransformed text calculating unit body is operative to calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and

the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the first untransformed text calculating unit; receive the putative untransformed text outputted; input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the second untransformed text calculating unit together with the plaintext; and optionally output the

46 recalculation request data to the first session key prospect calculating section in response to  
47 receipt of the uncalculability identifier data outputted from the second session key prospect  
48 calculating section to cause the first session key prospect calculating section to again calculate  
49 said another session key prospect for the immediately preceding round and then output the  
50 putative untransformed text based on said another session key prospect.

1